An overview of the Data Protection Act 2018

Contents

About ‘An overview of the Data Protection Act 2018’

This document is intended to summarise and explain the content and structure of the Data Protection Act 2018 (Act) for organisations and individuals who are already familiar with data protection law and the GDPR. It seeks to help you understand and navigate your way around the Act. However, it is vital that you continue to review the precise wording of the Act itself, when deciding how it may apply to any processing of personal data.

It is not intended to contain practical guidance on your obligations. If you are looking for a general introduction to data protection law, or for guidance on how these provisions operate in practice and on how to comply, please see our Guide to Data Protection.

The Act can appear to be a complex piece of legislation as it brings together four regimes of data protection law. In practice, most organisations will be concerned with only the two ‘general processing’ regimes in Part 2, which are intended to operate in a very similar manner. The other two regimes apply to a limited group of controllers: law enforcement ‘competent authorities’ and the intelligence services. Individuals may of course be affected by processing which is regulated under any one of the four regimes.

Background

What is the purpose of the Data Protection Act?

The Act seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data.

> "The previous Data Protection Act, passed a generation ago, failed to account for today's internet and digital technologies, social media and big data. The new Act updates data protection laws in the UK…[and]… provides tools and strengthens rights to allow people to take back control of their personal data."
>
> **Elizabeth Denham – Information Commissioner**

The Act came into force on 25 May 2018. The Act updates data protection laws in the UK, supplementing the General Data Protection Regulation (EU) 2016/679 (GDPR), implementing the EU Law Enforcement Directive (LED), and extending data protection laws to areas which are not covered by the GDPR or the LED. It provides a comprehensive package to protect personal data.

Why is the Act necessary?

The Act does not write the GDPR into UK law. The GDPR has direct effect in EU member states from 25 May 2018, which means the GDPR is already part of UK law. After the UK leaves the EU, the GDPR will be converted into UK law (with some amendments) under the European Union (Withdrawal) Act 2018.

However, the GDPR permits Member States to make some adaptations to reflect national requirements. The Act therefore adapts the GDPR, for example by providing some specific conditions for processing sensitive data, and some exemptions specific to the UK. It also provides for regulation and enforcement in the UK.

The Act also implements the LED regime for competent authorities processing for law enforcement purposes. The LED as an EU directive does not have direct effect, and requires national law to implement it.

In addition, the Act extends GDPR standards to areas of processing not covered by the GDPR or LED. It also creates a specific data protection regime for the intelligence services, based on the standards in the modernised Convention 108 (the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

Structure of the Act

The Act plays a key role in implementing a wide range of data protection reforms across the UK.

The Act introduces four distinct data protection regimes into UK Data Protection law. Each regime focuses on the regulation of personal data processing for a specific type or category of data processing. The four regimes cover processing:

- within the scope of the GDPR;
- outside the scope of the GDPR;
- by competent authorities for law enforcement purposes; and
- by the intelligence services.

The Act is split up into seven parts and multiple schedules:

Section	Section title	Overview of section
Part 1	Preliminary	• Overview of the Act. • Key terms used in the Act.
Part 2	General Processing	• Applies to most processing of personal data in the UK. • Split into two parts. First under the GDPR and second applying a similar regime to processing not covered by the GDPR, Part 3 for Law Enforcement or Part 4 for Intelligence Services.
Part 2, Chapter 2	General Processing - The GDPR	• Applies to processing of personal data to which the GDPR applies. • Supplements and must be read with the GDPR. • Addresses areas left for Member State implementation under the GDPR. • Refers to Schedules 1 to 4.
Part 2, Chapter 3	General Processing - Other General Processing	• Applies to processing of personal data to which the GDPR does **not** apply. • It does not apply to law enforcement processing or intelligence service processing. • Referred to in the Act as the **applied GDPR**. • Also applies Part 2 Chapter 2 (along with the

Section	Section title	Overview of section
		relevant Schedules) to the applied GDPR.
Part 3	Law Enforcement Processing (LE processing)	• Transposes the LED into UK law. • Addresses areas left for Member State implementation under the LED. • Applies the same regime to UK law enforcement processing not covered by the LED.
Part 4	Intelligence Service Processing (IS processing)	• Provides intelligence services with a specific data protection regime for the processing of personal data.
Part 5	The Information Commissioner	• Details the general functions of the Information Commissioner and her office, along with her powers. • Provides information about the international role of the Information Commissioner. • Provides information about the statutory guidance which the Information Commissioner produces.
Part 6	Enforcement	• Sets out the enforcement regime under the Act. • Provides details about the notices the Information Commissioner can issue. • Provides information about offences, claims, appeals and complaints.
Part 7	Supplementary and Final Provision	• Additional provisions, eg additional information about offences, the Tribunal, the territorial application of the Act and further definitions.
Schedule 1	Special categories of personal data and criminal convictions etc data	• Provides a list of conditions which, if one is met, permit the processing of the special categories of personal data and criminal conviction data.

Section	Section title	Overview of section
		• Details policy documentation and additional safeguards which must be put in place when relying on some of the conditions listed. • These apply to the GDPR and applied GDPR.
Schedule 2	Exemptions etc from the GDPR	• Provides various exemptions (permitted under GDPR). This applies to the GDPR and applied GDPR.
Schedule 3	Exemptions etc from the GDPR: health, social work, education and child abuse data	• Provides exemptions (permitted under GDPR) for health, social work, education and child abuse data. This applies to the GDPR and the applied GDPR.
Schedule 4	Exemptions etc from the GDPR: disclosure prohibited or restricted by an enactment	• Provides exemptions (permitted under GDPR) where disclosure is prohibited or otherwise restricted by an enactment. For example, relating to adoption records. This applies to both the GDPR and the applied GDPR.
Schedule 5	Accreditation of certification providers: reviews and appeals	• Provides details as to when and how a review or appeal can be made about the accreditation of certification providers.
Schedule 6	The applied GDPR and the applied Chapter 2	• Modifies the applied GDPR and applied Chapter 2 so that it makes sense in a UK only context. For example, making changes to territorial application and co-operation with other supervisory authorities.
Schedule 7	Competent authorities	• Provides a list of the "competent authorities" referred to in Part 3 (LED processing).
Schedule 8	Conditions for sensitive processing under Part 3	• Provides conditions which must sometimes be met before carrying out sensitive processing by competent authorities under Part 3 (LED processing).
Schedule 9	Conditions for processing under Part 4	• Provides conditions which must be met before personal data can be processed under Part 4 (IS processing).

Section	Section title	Overview of section
Schedule 10	Conditions for sensitive processing under Part 4	• Provides conditions which must be met before sensitive processing can be carried out by the intelligence services under Part 4 (IS processing).
Schedule 11	Other exemptions under Part 4	• Provides exemptions which may apply under Part 4 (IS processing
Schedule 12	The Information Commissioner	• Provides for the operation of the Information Commissioner's Office, addressing areas such as the appointment of the Information Commissioner and the resourcing of her office.
Schedule 13	Other general functions of the Commissioner	• Provides for other general functions of the Information Commissioner, such as those relating to Part 3 (LED processing) and Part 4 (IS processing).
Schedule 14	Co-operation and mutual assistance	• Provides for the Information Commissioner's role in ensuring co-operation and mutual assistance with LED supervisory authorities and foreign designated authorities.
Schedule 15	Powers of entry and inspection	• Provides for the Information Commissioner's powers of entry and inspection.
Schedule 16	Penalties	• Details the content of notices concerning penalties and the enforcement of payments.
Schedule 17	Review of processing of personal data for the purposes of journalism	• Provides further detail of the Information Commissioner's information and assessment notices powers, in relation to undertaking a review of processing of personal data for the purposes of journalism.
Schedule 18	Relevant Records	• Provides definitions and further provisions relating to relevant records – that is health records, records relating to a conviction or caution, or records relating to statutory functions.

Section	Section title	Overview of section
Schedule 19	Minor and consequential amendments	• Details amendments to other legislation.
Schedule 20	Transitional Provision etc	• Details the transition of provisions relating to previous data protection legislation to the adoption of the Act.

Part 1, Data Protection Act

Preliminary

What is the scope of Part 1?

Part 1 sets out definitions that are used throughout the Act. These definitions closely reflect those found in the GDPR, although there are some minor differences. Of course these definitions do not apply when these terms are used within the GDPR.

Key terms	Definition
Personal data	Any information relating to an identified or identifiable living individual. This definition does not include the extra detail in the GDPR which goes on to define an 'identifiable living individual'.
Identifiable living individual	A living individual who can be identified, directly or indirectly, in particular by reference to: • an identifier such as a name, an identification number, location data or an online identifier; or • one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
Processing	In relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as: • collection, recording, organisation, structuring or storage; • adaptation or alteration; • retrieval, consultation or use; • disclosure by transmission, dissemination or otherwise making available; • alignment or combination; or • restriction, erasure or destruction.
Data subject	The identified or identifiable living individual to whom personal data relates.

1 Part 1, Data Protection Act

Key terms	Definition
Controller and processor	Part 1 does not provide a single definition of controller and processor. Instead it points to the relevant Chapter or Part of the Act for the specific definition of these terms. As a general rule the definitions of controller and processor mirror those of the GDPR: • 'controller' means the natural or legal person who alone or jointly with others determines the purpose and means of the processing of personal data; and • 'processor' means the natural or legal person who processes personal data on behalf of the controller.
Filing system	Any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.
The applied GDPR	The GDPR as applied by Part 2 Chapter 3. In practice this means that the Act extends GDPR standards to: • processing outside the scope of EU law • processing outside the scope of the GDPR other than processing covered by Part 3 (LED processing) or Part 4 (IS processing).

There is a useful index of definitions and interpretations within the Act at Section 204 to 206.

Part 2, Data Protection Act

General processing

What is the scope of Part 2?

Part 2 has two key purposes. The first is to supplement the GDPR by completing sections that have been left open for Member State interpretation and implementation. The second is to apply the GDPR requirements to certain general processing that falls outside its scope.

Given the connection between Part 2 of the Act and the GDPR, it is important to read both of these together when considering how to implement data protection requirements.

Part 2, Chapter 1 sets out the scope and some definitions.

Part 2, Chapter 2 applies to the same types of processing that the GDPR applies to. If the processing is subject to the requirements of the GDPR, then Part 2, Chapter 2 will apply to that processing.

Part 2, Chapter 3 generally applies to processing of personal data that falls outside of the scope of EU law and the GDPR and which is not Part 3 LED processing or Part 4 IS processing. For example, the manual processing of unstructured personal data, such as unfiled handwritten notes on paper, by those public authorities that are subject to the information access regime under the Freedom of Information Act 2000.

Chapters 2 and 3 do not apply to processing of personal data by an individual for a purely personal or household activity.

Chapter and title	Overview of chapter content
1. Scope and definitions	• Sets the scope of Part 2, Chapters 2 and 3. • Describes how to interpret definitions from the GDPR when reading Chapters 2 and 3.

2 Part 2, Data Protection Act

Chapter and title	Overview of chapter content
2. The GDPR	• Defines and modifies certain terms used in the GDPR. • Describes five lawful bases of processing which are considered necessary in the public interest or for the exercise of a controller's official authority. • Provides for children aged 13 and over to give consent for information society services. • Sets out when the processing of the special categories of personal data and personal data relating to criminal convictions and offences and related security measures is permitted. • Provides for special obligations for credit reference agencies in relation to the data subject's right of access. • Makes provision for automated decision-making authorised by law. • Establishes exemptions to rights and obligations under the Act. • Makes provision for the accreditation of certification providers. • Makes provision for the transfer of personal data outside the EU. • Makes provision for processing for archiving, research and statistical purposes.
3. Other General Processing	• Sets out the scope of Chapter 3 and definitions used in the Chapter. • Describes how the GDPR applies to processing activities within the scope of Chapter 3. • Describes how Chapter 2 (and also the Schedules referred to in Chapter 2) apply to processing under the applied GDPR, as they apply to processing under the GDPR. • Modifies the text of the GDPR and Chapter 2 to work in a purely national context, by reference to Schedule 6. • Sets out exemptions from the GDPR provisions for manual unstructured data held by public authorities subject to Freedom of Information Act obligations. • Sets out modifications and exemptions from the application of the GDPR for personal data processed for national security and defence purposes.

Part 2, Chapter 2 - The GDPR

What terms are specific to Part 2, Chapter 2 and what do they mean?

Generally, the terms used in Part 2, Chapter 2 have the same meaning as they do in the GDPR. However in certain instances, terms from the GDPR are modified, clarified or are given a different meaning, including those in the table below.

Term	Overview of term
Controller	This clarifies that where personal data is processed, for purposes and means that are required by an enactment, the person who is obliged to undertake this processing, by the enactment, will be the controller. The definition also identifies particular bodies and persons that act on behalf of the Crown and Parliament as data controllers.
Public authority and public body	A definition for the terms "public authority" and "public body" are set out for the purposes of interpreting the GDPR. These terms are not defined in the GDPR itself. The Act provides that public authorities and public bodies are those defined by the Freedom of Information Act 2000, the Freedom of Information Act (Scotland) 2002 and any authority or body specified or described by the Secretary of State in regulations. However, such an authority or body will only be public body or authority for the purposes of the GDPR when performing a task carried out in the public interest or in the exercise of official authority vested in it. In addition, the Act confirms that certain authorities, such as a parish council in England, or a community council in Wales or Scotland, will not fall within the definition of "public authority" or "public body" within this Part of the Act.
Personal data relating to criminal convictions and offences or related security measures	The Act clarifies that such data includes personal data relating to: (a) the alleged commission of offences by the data subject; or (b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing. In this document, we refer to this type of personal data as "criminal convictions data". Please note, however, that criminal convictions data is not a formal definition used by the Act.
Court	The Act clarifies that, in relation to Chapter 2, Part 2, the term "court" does not include a tribunal.

What is the scope of Part 2, Chapter 2?

The GDPR establishes a pan-European regime for the general processing of personal data. The Regulation has direct effect (ie it applies in all Member States without the need for it to be implemented by national legislation) from May 2018. This means that the Act does not need to re-state the GDPR as it is applies in the UK in any event.

The GDPR recognises that there are differences in the legal, economic and social environments of the Member States. In specific instances it expressly allows Member States to derogate from or supplement the GDPR to accommodate these national differences. The Act operates with the GDPR and sets out the derogations and supplementing provisions that have effect in the UK.

Some of the key areas addressed by the Act to tailor the GDPR to the UK environment are:

Lawfulness of processing: public interest, etc

The GDPR prohibits the processing of personal data unless the controller is able to identify an appropriate legal basis for that processing. Article 6(1) of the GDPR sets out six lawful bases for processing and, under Article 6(2), Member States are permitted to introduce more specific provisions for these six bases.

> **GDPR Article 6(1)(e):** permits processing where necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

> **Act Section 8:** a task carried out in the public interest or the exercise of official authority includes processing that is necessary for the: (a) administration of justice; (b) exercise of a function of either House of Parliament; (c) exercise of a function conferred on a person by an enactment or rule of law; (d) exercise of a function of the Crown, a Minister of the Crown or a government department; or (e) an activity that supports or promotes democratic engagement.

Child's consent in relation to information society services

GDPR Article 8: where consent is relied on as the lawful ground for processing the personal data of a child, as part of an "information society service", consent will only be valid if the child is at least 16 years old.

The term "information society service" refers to "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"(see Article 1 of Directive (EU) 2015/1535).

Act Section 9: the UK has applied a lower age limit for gaining valid consent from children when offering an information society service. In the UK consent is valid from children of at least 13 years old.

Special categories of personal data and criminal offence data

GDPR Articles 9 and 10: The GDPR requires special conditions to be met for processing "special categories" of personal data and criminal offence data. Articles 9 and 10 of the GDPR prohibit the processing of such data unless the special conditions, set out in Articles 9(2) and 10 respectively, are met.

The special categories are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The special conditions which allow processing of special category personal data include these five which each require a further basis in UK law:

- Article 9(2)(b) – for employment, social security and social protection purposes.
- Article 9(2)(g) – for substantial public interest purposes.
- Article 9(2)(h) – for health and social care purposes.
- Article 9(2)(i) – for public health purposes.
- Article 9(2)(j) – for archiving, research and statistical purposes.

Article 10 requires that the processing of criminal offence data is

prohibited unless it is carried out under the control of official authority or if it is authorised by EU or UK law providing for appropriate safeguards for the rights and freedoms of data subjects.

Act Section 10 and Schedule 1: set out when processing of the special categories of personal data and criminal offence data has the relevant authorisation in UK law. Section 10 and Schedule 1 combine to set out additional conditions that must be met and safeguards that must be put in place.

Schedule 1 – Conditions relating to the processing of the special categories of personal data and criminal convictions (etc) data

Schedule 1 of the Act establishes conditions that permit the processing of the special categories of personal data and criminal offence data.

The Schedule is split into four parts.

- Part 1 – Conditions relating to employment, health and research
- Part 2 – Substantial public interest conditions
- Part 3 – Additional conditions relating to criminal offence data
- Part 4 – Appropriate policy document and additional safeguards

Processing of the special categories of personal data meets the requirements in points (b), (h), (i) or (j) of Article 9(2) of the GDPR (for authorisation by, or a basis in UK law) if it meets one of the conditions listed in Part 1 of Schedule 1.

Processing of the special categories of personal data meets the requirement in point (g) of Article 9(2) of the GDPR (for a basis in UK law) if it meets one of the conditions listed in Part 2 of Schedule 1.

Processing meets the requirement in Article 10 of the GDPR (for authorisation by UK law) if it meets one of the conditions listed in Part 1, 2 or 3 of Schedule 1.

Schedule 1, Part 1 conditions - processing in connection with employment, health and research

- Employment, social security and social protection
  Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection. In order to meet this condition the controller must have an

appropriate policy document in place, as required under Part 4 of Schedule 1 (see further guidance on appropriate policy documentation on page 24)

- Health or social care
  Processing necessary for health or social care purposes.

- Public health
  Processing necessary for reasons of public interest in the area of public health, and carried out under the responsibility of a health professional or another person who owes a duty of confidentiality under enactment or rule of law.

- Research
  Processing necessary for archiving purposes, scientific or historical research purposes or statistical purposes, carried out in the public interest and in accordance with Article 89(1) GDPR (as supplemented by s19 of the Act) .

Schedule 1, Part 2 conditions - processing in the substantial public interest

- Statutory and government purposes
  Processing necessary for the exercise of a function conferred on a person by enactment or rule of law or the exercise of a function of the Crown, a Minister or a government department.

- Administration of Justice and parliamentary purposes
  Processing necessary for the administration of justice or the exercise of a function of either House of Parliament.

- Equality of opportunity or treatment
  Processing necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people with the view to enabling such equality to be promoted or maintained.

  It only applies to particular types of special category data, and the Act sets out in a table the type of review which can be conducted. For example, data concerning sexual orientation can only be processed for reviewing equality of opportunity or treatment of people of different sexual orientation.

  It does not apply if the processing is for the purposes of measures or decisions with respect to a particular data subject or if it is likely to cause substantial damage or substantial distress to an individual, or if a data

subject has given written notice to the controller not to process the data and a reasonable time has passed.

- Racial and ethnic diversity at senior levels of organisation
  Processing of personal data revealing racial or ethnic origin to allow organisations to identify suitable individuals to hold senior positions (ie a director), where such processing is necessary to promote or maintain diversity and can reasonably be carried out without the data subject's consent

  This does not apply where the processing is likely to cause substantial damage or distress to an individual.

- Preventing or detecting unlawful acts
  Processing necessary to prevent or detect an unlawful act (including an unlawful failure to act) that must be carried out without the data subject's consent.

- Protecting the public against dishonesty etc
  Processing which must be carried out without the data subject's consent, to protect the public against:
  - dishonesty, malpractice or other serious improper conduct;
  - unfitness or incompetence;
  - mismanagement in the administration of a body or association; or
  - failures in services provided by a body or association.

- Regulatory requirements relating to unlawful acts and dishonesty etc
  Processing which must be carried out without the data subject's consent and is necessary to comply, or assist other persons to comply, with a regulatory requirement, which involve taking steps to establish whether a person has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct.

- Journalism etc in connection with unlawful act and dishonesty etc The disclosure of personal data for the "special purposes" (journalistic, academic, artistic and literary purposes), in relation to matters (whether alleged or established) concerning:
  - the commission of an unlawful act by a person;
  - dishonesty, malpractice or other serious improper conduct;
  - unfitness or incompetence;
  - mismanagement in the administration of a body or association; or

  - failures in services provided by a body or association
  - And carried out with a view to the publication of personal data,

- Preventing fraud
  Certain specified processing for the purposes of preventing fraud.

- Suspicion of terrorist financing and money laundering
  Processing necessary for certain disclosures made under the Terrorism Act 2000 and Proceeds of Crime Act 2002.

- Support for individuals with a particular disability or medical condition
  Processing of certain types of personal data (eg genetic or biometric data) necessary for the purposes of raising awareness of the disability or medical condition, or providing support to those impacted by the disability, when undertaken by a not-for-profit body which provides support to individuals with that particular disability or medical condition.

- Counselling etc
  Processing necessary for the provision of confidential counselling, advice or support services that must be carried out without the consent of the data subject.

- Safeguarding of children and of individuals at risk
  Processing necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm or protecting their physical, mental or emotional well-being, where the individual is under 18 years old or over 18 and at risk.

- Safeguarding of economic well-being of certain individuals
  Processing of data concerning health necessary for the protection of the economic well-being of an individual at economic risk who is aged 18 or over and must be carried out without the data subject's consent for certain specified reasons..

- Insurance
  Processing necessary for an insurance purpose, and which is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health that can reasonably be carried out without the data subject's consent and is not for the purpose of measures or decisions with respect to the data subject.

- Occupational pensions
  Processing of health data, which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme, and where such processing is necessary for the purpose of making

a determination in connection with eligibility for or benefits payable under, an occupational pension scheme, cannot reasonably be carried out with the data subject's consent and is not for the purpose of measures or decisions with respect to the data subject .

- Political parties
  Processing of political opinions data necessary for the political activities of a person or organisation registered under s.23 Political Parties, Elections and Referendums Act 2000 that would not be likely to cause substantial damage or substantial distress .

  this does not apply where a data subject has given written notice to the controller not to process the data and a reasonable time has passed.

- Elected representatives responding to requests
  Allows an elected representative or someone acting on his behalf to process data where necessary (in connection with the discharge of the elected representative's functions)
  for the purpose of taking action in response to a request from an individual.

- Disclosure to elected representative
  Processing which consists of the disclosure of personal data to an elected representative or a person acting on his behalf by a data controller necessary for the purpose of
  responding to a communication from the representative (in relation to a request the representative has received from an individual).

- Informing elected representatives about prisoners
  Processing for the purpose of informing a member of the House of Commons or a member of the Scottish Parliament about a prisoner.

- Publication of legal judgments
  Processing which is necessary for the purpose of publishing a judgment or other decision of a court or tribunal.

- Anti-doping in sport
  Processing which is necessary: (i) in connection with measures designed to eliminate (identify or prevent) doping which are undertaken by a body with responsibility for eliminating doping; or (ii) for the purpose of providing information about doping or suspected doping to such a body.

- Standards of behaviour in sport
  Processing which must be carried out without the data subject's consent, where it is necessary to protect the integrity of a sport or sporting event from dishonesty, malpractice or other seriously improper

conduct, or failure by a person participating in the sport or event to comply with standards of behaviour set by a body or association with responsibility for the sport or event.

Part 2, paragraph 5 provides that, in most instances, in order to meet a condition in this part the controller must have an appropriate policy document in place, as required under Schedule 1, Part 4.

Schedule 1, Part 3 conditions – processing criminal convictions data

- Consent
  Processing with the consent of the data subject.

- Protecting individual's vital interests
  Processing of criminal convictions data necessary in the vital interests of an individual and the data subject cannot consent.

- Processing by not-for-profit bodies
  Processing in the course of legitimate activities pursued by a not-for-profit body with a political, philosophical, religious or trade union aim where the processing relates to members, former members or persons with regular contact with the body.

- Personal data in the public domain
  Processing where personal data is manifestly made public by a data subject.

- Legal claims
  Processing is necessary for purpose of: (i) any legal proceedings; (ii) obtaining legal advice; or (iii) establishing, exercising or defending legal rights.

- Judicial acts
  Processing is necessary when a court or tribunal is acting in its judicial capacity.

- Administration of accounts used in commission of indecency offences involving children
  Processing for certain indecency offences processing involving children necessary for administering an account relating to the payment card used in the commission of the offence or cancelling the card used. In order to meet this condition the controller must have an appropriate policy document in place, as required under Part 4 of Schedule 1 (see further guidance on appropriate policy documentation on page 24).

- Extension of certain conditions under Schedule 1, Part 2
  Allows processing of criminal convictions data, where processing would

meet a condition in Schedule 1, Part 2 except for the fact it must satisfy the substantial public interest test.

- Extension of insurance conditions
  Should the processing of personal data not reveal racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, then this extension allows processing where it would otherwise meet the insurance condition in Schedule 1, Part 2, or the condition relating to the extension of certain conditions under Schedule 1, Part 2 stated above (when processing criminal convictions data).

Part 4 – Appropriate policy documentation and additional safeguards

Schedule 1, Part 4 makes provision for the establishment, content and maintenance of "appropriate policy documentation" where such documentation is required by a condition in Parts 1, 2 or 3.

This appropriate policy documentation must:

- explain how the controller complies with the data protection principles set out in Article 5 of the GDPR;
- explain the controller's policies for the retention and erasure of personal data processed under the relevant condition; and
- be retained, reviewed and (if appropriate) updated by the controller and (if requested) made available to the Information Commissioner, until six months after the controller ceases carrying out the processing.

Where appropriate policy documentation is required, the controller's records of processing activities (under Article 30 of the GDPR) must include:

- details of the relevant condition relied on;
- how processing satisfies Article 6 of the GDPR (lawfulness of processing); and
- details of whether the personal data is retained and erased in accordance with the appropriate policy documentation (and if not the reasons why not).

Obligation of credit reference agencies

> **GDPR Article 15**: This provides data subjects with a right of access to personal data held about them by a controller.

Act Section 13: limits the extent to which the right of access applies to credit reference agencies. Credit reference agencies are only required to include personal data about a data subject's financial standing when responding to a subject access request, unless the data subject indicates otherwise.

When responding to a subject access request, credit reference agencies are also required to inform data subjects of their right to have incorrect information corrected under the Consumer Credit Act 1974.

Automated decision-making authorised by law: safeguards

GDPR Article 22: This requires that data subjects shall not be subject to a decision based solely on automated processing (including profiling), which produces legal effects concerning the data subject or similarly affects them.

This will not apply if the automated decision making is authorised by EU or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Act Section 14: sets out the safeguards that must be in place when a significant decision is based solely on automated processing which is required or authorised by law:

- the controller must notify the data subject, as soon as reasonably practicable, that a decision has been taken based solely on automated processing;
- the data subject is given 1 month from receipt of the notification to request the controller either to reconsider the decision, or take a decision that is not based solely on automated processing; and
- from receipt of the request from the data subject, the controller has 1 month (or 3 months should the request be complex if there are a number of them to comply with the request and notify the data subject in writing of the steps taken to comply with the request and the outcome of complying.

Exemptions

GDPR Article 23: This permits EU or Member State legislation to restrict the scope of obligations and rights under the GDPR where such restriction is necessary to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- other important objectives of general public interest of the EU or of a Member State, in particular an important economic or financial interest, public health and social security;
- the protection of judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- monitoring, inspection or regulatory function connected with the exercise of official authority related to national security, important objectives of general public interest and the prevention, investigation detection and prosecution of breaches of ethics in regulated professions;
- the protection of data subjects or the rights and freedoms of others; and
- the enforcement of civil law claims.

In addition **Article 85** permits certain exemptions from the GDPR for reasons relating to freedom of expression and **Article 89** permits exemptions from the GDPR for reasons relating to scientific or historical research purposes, statistical purposes and archiving purposes. These are discussed further below.

Act Section 15 and Schedules 2, 3 and 4: set out the exemptions from the GDPR, in accordance with Articles 23, 85 and 89 of the GDPR.

2 Part 2, Data Protection Act

The tables below lists the exemptions in the Act and the relevant Articles of the GDPR they can exempt you from. However, these exemptions will not apply in every case, and may only apply to some extent. See our Guide to Data Protection for more detail and for guidance on applying the exemptions.

For your ease of reference, the relevant GDPR Articles are:

Article 5: the Principles
Article 13: Transparency information when collecting personal data directly
Article 14: Transparency information when not collecting personal data directly
Article 15: Subject access
Article 16: Right of rectification
Article 17: Right to erasure
Article 18: Right to restriction of processing
Article 19: Notification regarding rectification, erasure or restriction
Article 20: Right of data portability
Article 21: Right to object
Article 34: Communication of a personal data breach to the data subject

Exemption	GDPR Article										
	5	13	14	15	16	17	18	19	20	21	34
Crime and taxation: general Schedule 2, Para 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Crime and taxation: risk assessment system Schedule 2, Para 3	✓	✓	✓	✓							
Immigration Schedule 2, Para 4	✓	✓	✓	✓		✓	✓			✓	

2 Part 2, Data Protection Act

Exemption	GDPR Article										
	5	13	14	15	16	17	18	19	20	21	34
Information required to be disclosed by law etc or in connection with legal proceedings **Schedule 2, Para 5**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Functions designed to protect the public etc **Schedule 2, Para 7**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Audit Functions **Schedule 2, Para 8**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Functions of the Bank of England **Schedule 2, Para 9**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Regulatory functions relating to legal services, the health service and children's services **Schedule 2, Para 10**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Regulatory functions of certain other persons **Schedule 2, Para 11**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Parliamentary privilege **Schedule 2, Para 13**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

2 Part 2, Data Protection Act

Exemption	GDPR Article										
	5	13	14	15	16	17	18	19	20	21	34
Judicial appointments, judicial independence and judicial proceedings **Schedule 2, Para 14**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Crown honours, dignities and appointments **Schedule 2, Para 15**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Protection of the rights of others **Schedule 2, Para 16**	✓			✓							
Legal professional privilege **Schedule 2, Para 19**	✓	✓	✓	✓							
Self-incrimination **Schedule 2, Para 20**	✓	✓	✓	✓							
Corporate finance **Schedule 2, Para 21**	✓	✓	✓	✓							
Management forecasts **Schedule 2, Para 22**	✓	✓	✓	✓							

2 Part 2, Data Protection Act

Exemption	GDPR Article										
	5	13	14	15	16	17	18	19	20	21	34
Negotiations Schedule 2, Para 23	✓	✓	✓	✓							
Confidential references Schedule 2, Para 24	✓	✓	✓	✓							
Exam scripts and exam marks Schedule 2, Para 25	✓	✓	✓	✓							
Journalistic, academic, artistic and literary purposes Schedule 2, Para 26	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Plus Articles 6, 7, 8, 9, 10, 11, 36, 44, and 60-67.										
Research and statistics Schedule 2, Para 27				✓	✓		✓			✓	
Archiving in the public interest Schedule 2, Para 28				✓	✓		✓	✓	✓	✓	
Health data processed by a court Schedule 3, Para 3	✓	✓	✓	✓	✓	✓	✓		✓	✓	

2 Part 2, Data Protection Act

Exemption	GDPR Article										
	5	13	14	15	16	17	18	19	20	21	34
Data subjects expectations and wishes with respect to health data **Schedule 3, Para 4**	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Serious harm from health data disclosure **Schedule 3, Para 5**				✓							
Social work data processed by a court **Schedule 3, Para 9**	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Data subjects expectations and wishes with respect to social work data **Schedule 3, Para 10**	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Serious harm from social work data disclosure **Schedule 3, Para 11**				✓							
Education data processed by a court **Schedule 3, Para 18**	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Serious harm from education data disclosure **Schedule 3, Para 19**				✓							

2 Part 2, Data Protection Act

Exemption	GDPR Article										
	5	13	14	15	16	17	18	19	20	21	34
Child abuse data **Schedule 3, Para 21**				✓							
Disclosures prohibited or restricted by an enactment: Human fertilisation and embryology information **Schedule 4, Para 2**	✓			✓							
Disclosures prohibited or restricted by an enactment: Adoption records and reports **Schedule 4, Para 3**	✓			✓							
Disclosures prohibited or restricted by an enactment: Statements of special educational needs **Schedule 4, Para 4**	✓			✓							
Disclosures prohibited or restricted by an enactment: Parental order records and reports **Schedule 4, Para 5**	✓			✓							
Disclosures prohibited or restricted by an enactment: Information provided by Principal Reporter for children's hearing **Schedule 4, Para 6**	✓			✓							

Accreditation of certification providers

GDPR Article 43: provides for the accreditation by a Member State's supervisory authorities or other national accreditation bodies of organisations wishing to operate as certification providers.

Act Section 17: the Information Commissioner and the UK's national accreditation body (UKAS) are the only persons who can provide accreditation of certification providers in the UK. Further, the Information Commissioner and UKAS may only accredit certification providers after the Information Commissioner has published a statement that they and, where applicable, UKAS, will undertake this accreditation role. Section 17 also confirms that UKAS may charge a reasonable fee in relation to accreditation.

Schedule 5 of the Act sets out the review and appeal process for accreditation decisions.

The GDPR encourages Member States and supervisory authorities, such as the Information Commissioner, to establish certification mechanisms and data protection seals and marks. These demonstrate compliance with data protection obligations by controllers and processors.

Transfers of personal data to third countries, etc

GDPR Articles 44 to 49: The GDPR imposes a general prohibition on the transfer of personal data outside the EU, unless:

- Article 45 - the transfer is based on an adequacy decision;
- Article 46 – the transfer is subject to appropriate safeguards;
- Article 47 – the transfer is governed by Binding Corporate Rules; or
- Article 49 – the transfer is in accordance with specific exceptions.

One of the specific exceptions is where the transfer of personal data outside the EU is necessary for important reasons of public interest (Article 49(1)(d)).

Act Section 18: permits the Secretary of State to specify circumstances where transfers will or will not be considered to be necessary for important reasons of public interest. In addition it permits the Secretary of State to restrict transfers out of the EU more generally where it is necessary for important reasons of public interest.

Processing for archiving, research and statistical purposes: safeguards

GDPR Articles 9(j) and 89(1): There is a specific legal basis for processing special categories of data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which is also in accordance with Article 89(1) and based on Member State law which contains suitable safeguards.

Act Section 19 sets out suitable safeguards for UK law, in that processing will not satisfy the safeguards requirement where it is:

- for measures or decisions with respect to a particular data subject, unless the purpose for which the processing is necessary includes the purposes of approved medical research; or
- likely to cause substantial damage or substantial distress to a data subject.

Part 2, Chapter 3 – Other General Processing

What is the scope of Part 2, Chapter 3?

The GDPR doesn't apply to all processing of personal data occurring in the UK. It doesn't cover processing which is:

- **outside the scope of EU law**, such as immigration issues relating to third-country nationals on humanitarian grounds;
- **outside the scope of the GDPR**, such as 'common foreign and security policy activities' (Article 2(2)(b) GDPR), or manual unstructured processing of personal data held by an FOI public authority.

To fill in those gaps the Act covers:

- Part 3 (LED processing);
- Part 4 (IS processing);
- Part 2, Chapter 3 ('everything else').

Processing of personal data under Part 2, Chapter 3 is governed by:

- the applied GDPR;
- as modified by the applied Chapter 2; and
- as modified by Schedule 6.

"**The applied GDPR**" is used to mean the GDPR as it applies to processing covered by Part 2, Chapter 3 (ie, processing not covered by the GDPR, LED processing or IS processing).

"**The applied Chapter 2**" is used to mean Part 2, Chapter 2 of the Act as it applies to processing covered by Part 2, Chapter 3

Schedule 6 modifies the applied GDPR and the applied Chapter 2 to make the provisions work in a national context. For example, Schedule 6 removes references to "the Union" and "Member States" and replaces them with references to the United Kingdom. Schedule 6 changes are included in the definitions above.

This is set out in Part 2, Chapter 3, Sections 21 and 22.

Which terms are specific to Part 2, Chapter 3 and what do they mean?

Part 2, Chapter 3 includes terms which are not used elsewhere in the Act, including the key terms in the table below.

Term	Overview of term
Automated or structured processing of personal data	Processing of personal data: a) wholly or partly by automated means; and b) other than by automated means of personal data that forms part of a filing system or is intended to form part of a filing system.
Manual unstructured processing of personal data	Any processing of personal data which is not automated or structured processing.
FOI public authority	A public authority as defined by the Freedom of Information Act 2000 and the Freedom of Information Act (Scotland) 2002.
Held by an FOI public authority	This term is defined by reference to the relevant provisions of the Freedom of Information Acts in the UK, but excludes information held by an intelligence service on behalf of an FOI public authority. It goes on to exclude personal data which section 7 of the Freedom of Information Act 2000 or section 7 of the Freedom of Information (Scotland) Act 2002, prevents those Acts applying to.

Manual unstructured data held by public authorities

Chapter 3, Section 24 relates only to the processing of manual unstructured data. Therefore it covers all manual documents held by a public authority, from a pile of papers on a desk to papers unsystematically kept in files.

A key reason for including this type of data in the Act is that access to it under FOIA is covered by the FOIA exemption for personal data. This allows public authorities to consider access requests which include personal data in line with the requirements of the Act.

As an aside, Schedule 19, paragraph 55 to 64 contain consequential amendments to FOIA. This includes at paragraph 58(8), a specific provision allowing FOI public authorities to apply the legitimate interests gateway when disclosing information under FOIA (as was the case under the 1998 Act).

It would be disproportionately onerous to apply all the GDPR requirements to this type of data. Section 24 of the Act exempts manual unstructured personal data held by public authorities from most provisions of the applied GDPR.

The key obligations under the 'applied GDPR' which continue to apply in most cases (with some exceptions) include:

- Article 5(1)(d) Principle of accuracy
- Article 5(2) Principle of accountability (but only in relation to Art 5(1)(d))
- Article 15 - Right of access by the data subject (but only where the data subject provides a description of the personal data requested or the estimated cost of compliance does not exceed any maximum set by the Secretary of State)
- Article 16 – Right to rectification
- Article 17 – Right to erasure
- Article 18 – Right to restrict processing
- Articles 24 – 43 Controller and processor obligations, including Art 32 – security of processing

Manual unstructured data used in longstanding historical research

Chapter 3, Section 25 covers historical research which has been running since before 24 October 1998, conducted by a FOI public authority.

In addition to the exemptions in Section 24 for an FOI public authority, the following are also excluded:

- Article 5(1)(d) - Principle of accuracy
- Article 16 – Right to rectification
- Article 17 – Right to erasure

National security and defence exemption

Chapter 3, Section 26 is an exemption for processing for national security and defence purposes, other than processing under the GDPR, or a law enforcement organisation (a 'competent authority') under Part 3 or by the intelligence services.

The key obligations under the 'applied GDPR' which continue to apply include:

- Article 5 in so far as it requires processing to be lawful under Article 6),
- Article 6.
- Article 9
- Articles 24 - 32 – controller and processor – including the security requirements but excluding personal data breach notification
- Articles 83 & 84 – administrative fines and penalties

Some key obligations which are excluded are:

- Chapter III GDPR – data subject rights
- Articles 33 & 34 – personal data breach notifications
- Chapter V – transfers to third countries and international organisations

Under Section 27 a Cabinet Minister, the Attorney General or the Advocate General for Scotland can sign a certificate that the exemption in Section 26 is required for safeguarding national security, and this certificate will be conclusive evidence. An affected data subject can appeal this to the Information Tribunal.

Section 28 modifies Article 9 of the GDPR, to allow processing of special category data for national security and defence purposes.

It also excludes Article 32, requirement on controllers and processors to put in place appropriate technical and organisational measures, when processing personal data for national security and defence purposes. Instead the controller or processor must simply comply with the requirement to put in place security measures appropriate to the risks arising from the processing of the personal data.

Part 3, Data Protection Act

Law enforcement processing

What is the scope of Part 3?

Part 3 is applies to people, bodies or organisations which are either specified in the Act or which have statutory functions for any of the law enforcement purposes and is relevant to all individuals whose personal data may be handled for those purposes.

Part 3 regulates the processing of personal data by competent authorities ("competent authorities") for the purposes of "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" (together "law enforcement purposes").

This Part implements the Law Enforcement Directive EU2016/680 (LED) into UK law, with additional provisions. The LED came into force in 2016 and EU member states had until May 2018 to adopt national legislation implementing its provisions.

Part 3 is divided into the six chapters described in the table below.

Chapter and title	Overview of chapter content
1. Scope and definitions	• Sets the scope to which Part 3 applies. • Provides definitions adopted by Part 3.
2. Principles	• Sets out the six data protection principles, along with various safeguards which must be adhered to. All six of these principles must be met for a controller to comply with Part 3. The principles are similar but not identical to the GDPR principles.
3. Rights of data the data subject	• Provides individuals with a series of rights which they may exercise against controllers.
4. Controller and Processor	• Imposes a range of obligations upon controllers and processors, including the requirement to appoint a data protection officer.

3 Part 3, Data Protection Act

5. Transfers of Personal Data to Third Countries	• Establishes how and when personal data can be transferred to a third country outside the EU or an international organisation.
6. Supplementary	• Provides supplementary provisions such those relating to national security certificates and how infringements of Part 3 should be reported.

For more detailed guidance on these provisions, see our Guide to Law Enforcement Processing.

Part 4, Data Protection Act

Intelligence services processing

What is the scope of Part 4?

Part 4 is mainly of interest to the intelligence services and anyone whose personal data is or maybe processed by the intelligence services.

National security falls outside the scope of EU law. The activities of the UK intelligence services are therefore outside the scope of the GDPR and the LED. To address this, Part 4 of the Act introduces a data protection regime applicable to processing of personal data by the intelligence services, namely:

- the Security Service;
- the Secret Intelligence Service; and
- the Government Communications Headquarters.

Part 4 is based on the Council of Europe's modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("modernised Convention 108"). The original Convention 108 was opened for signature on 28th January 1981 and presently has 51 signatory countries. The modernised Convention 108 builds on the internationally recognised standards for personal data protection established under the original Convention.

Part 4 applies to the processing of personal data by intelligence services either (wholly or partly) by automated means or as part of (or intended to form part of) a filing system. It contains six chapters.

Chapter and title	Overview of chapter content
1. Scope and definitions	• Sets the scope to which Part 4 applies. • Provides definitions adopted by Part 4.
2. Principles	• Sets out six data principles, along with various safeguards which must be adhered to. All six of these principles must be met in order for a controller to comply with Part 4.
3. Rights of the data subject	• Provides data subjects with a series of rights which they may exercise against controllers.
4. Controller and Processor	• Imposes a range of obligations upon controllers and processors including data security and data breach obligations.
5. Transfers of	• Establishes when personal data can be transferred

4 Part 4, Data Protection Act

Chapter and title	Overview of chapter content
personal data outside the United Kingdom	outside the United Kingdom or to an international organisation.
6 Exemptions	• Provides exemptions where the provisions of this Part do not apply due to the requirement to safeguard national security.

Part 4, Chapter 1 - Scope and definitions

What terms are specific to Part 4?

The following key definitions are used:

Defined term	Simplified definition
Intelligence Service	• The Security Services; • The Secret Intelligence Service; and • The Government Communications Headquarters.
Controller	This means the intelligence service which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor	Any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).
Consent	This definition is largely taken from Recital 32 of the GDPR. Consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes. This must be provided by a statement or clear affirmative action, signifying the individual's agreement to the processing of their personal data.
Employee	In relation to any person, includes an individual who holds a position (whether paid or unpaid) under the direction and control of that person.
Sensitive processing	In essence, this is processing of special categories of data (as defined in the GDPR) plus processing of criminal convictions data.

In addition Chapter 1 provides definitions for a "personal data breach", "recipient" and "restriction of processing".

Part 4, Chapter 2 – Principles

Chapter 2 sets out six data principles, along with various safeguards which must be adhered to.

All six of these principles must be met in order to comply with Part 4.

The six data protection principles are as follows:

- first data protection principle – processing must be lawful, fair and transparent;
    - for processing to be lawful at least one of the Schedule 9 conditions must be met and in addition, for sensitive processing at least one of the Schedule 10 conditions.
- second data protection principle – purposes of processing must be specified, explicit and legitimate;
- third data protection principle – personal data must be adequate, relevant and not excessive;
- fourth data protection principle – personal data must be accurate and kept up to date;
- fifth data protection principle – personal data must be kept for no longer than is necessary; and
- sixth data protection principle –personal data must be processed in a secure manner.

Part 4, Chapter 3 – Rights of the data subject

Key rights	Overview of requirements
Right to information	• A controller must provide a data subject with the following information: ○ the identity and contact details of the controller; ○ the legal basis on which and the purposes for which their personal data is being processed; ○ the categories of personal data being processed; ○ the recipients or categories of recipients of the personal data; ○ the right to lodge a complaint with the Information Commissioner; ○ how to exercise their rights; and ○ any other information that is required to make processing fair. • The controller may comply with the right to information by making information generally available.
Right of access	• A data subject has the right to request confirmation from a controller whether or not their personal data is being processed and, if this personal data is being processed, access to their personal data and the information set out below: ○ the purpose and legal basis for the processing; ○ the categories of personal data concerned; ○ the recipients or categories of recipients to whom the personal data has been disclosed; ○ the period for which the personal data is to be preserved; ○ the existence of data subject's rights to rectification and erasure of personal data; ○ the right to lodge a complaint with the Information Commissioner; and ○ any information about the origin of the personal data.
Right not to be subject to automated	• A controller may not take a decision significantly affecting a data subject that is based solely on automated processing. • A decision will be considered to significantly affect a data subject if it has a legal effect concerning a data subject. A decision may

Key rights	Overview of requirements
decision-making	be made based solely on automated processing where: ○ it is authorised by law; ○ the data subject has given consent to the decision being made on that basis; or ○ a decision is taken for the purpose of considering whether to enter into a contract, or with a view to entering into a contract with the data subject or in the course of performing such a contract.
Right to object to processing	• A data subject may give notice to the controller requesting that the controller no longer process their personal data, either in general or for a specific purpose or in a specific manner. This notice may be given when an individual believes that this processing would cause an unwarranted interference with their rights.
Rights to rectification and erasure	• A data subject has the right to apply to court, where they believe their personal data is inaccurate, requesting that this is rectified without undue delay. • Likewise it is possible for a data subject to apply to court, where they believe that data protection principles have not been complied with, and for a court to order erasure of that data without undue delay. • A data subject may contest the accuracy of personal data held by a controller and a court may order that the processing of the personal data is restricted, where it is not possible for the controller to confirm the accuracy of the personal data.

Part 4, Chapter 4 – Controller and processor

What are the main obligations of a controller under Chapter 4?

A controller must implement appropriate measures to ensure that the processing of personal data complies with the requirements of Part 4. A controller must be able to evidence these measures to others, including the Information Commissioner.

A controller must also, prior to processing personal data, consider the impact of the proposed processing on the rights and freedoms of data subjects.

A controller must implement appropriate technical and organisational measures to ensure that the data protection principles are implemented and the risks to the rights and freedoms of data subjects are minimised.

There are provisions for joint controllers, with similar requirements to those in the GDPR.

What are the main obligations of a processor under Part 4?

A processor may only process personal data under this Part 4 on instruction from the controller or where complying with a legal obligation. It must also implement the security and data breach reporting measures described below.

What level of security does a controller or processor need to implement?

Each controller and processor must implement appropriate technical and organisational measures to ensure an appropriate level of security. Detailed obligations apply where there is automated processing.

What action does a controller need to take in the event of a data breach?
• Provide a notification to the Information Commissioner without undue delay. • If the notification is not made within 72 hours, the notification must detail the reason for the delay.
The notification must include: • a description of the nature of the data breach (eg approximate numbers of affected data subjects, the categories and approximate number of data records

What action does a controller need to take in the event of a data breach?

concerned etc);

the name and contact details of a contact point from whom additional information can be obtained;

- a description of the likely consequences of the breach; and
- a description of the measures taken by the controller to address the breach, including any measures to mitigate the adverse effects.

The information required for a notification may be provided in phases if it is not possible to provide this at the same time.

If a processor becomes aware of a data breach this must be communicated to the controller without undue delay.

Part 4, Chapter 5 – Transfers of personal data outside the United Kingdom

A controller may not transfer personal data to a country outside the United Kingdom or to an international organisation unless the transfer is necessary and proportionate for the purposes of that controller's statutory function or for purposes provided for in the relevant sections of the Security Services Act 1989 or the Intelligence Services Act 1994.

Part 4, Chapter 6 – Exemptions

Exemptions from certain provisions of the Act (as described below) apply to processing by the Security Services, if that exemption is required for the purpose of safeguarding national security:

- The data protection principles, except that the processing of personal data must remain lawful, and meet at least one of the conditions found in Schedule 9 for processing of personal data and Schedule 10 for sensitive processing.
- The rights of the data subject.
- The communication of a personal data breach to the Information Commissioner.
- Provisions relating to inspection of personal data in accordance with international obligations found in Part 5 of the Act.
- Certain powers of the Information Commissioner to monitor, enforce and conduct investigations.
- The Information Commissioner's power to issue notices and her powers of entry and inspection as found in Part 6 and Schedule 15 of the Act.
- The offences relating to personal data as found in Part 6.
- Provisions relating to the special purposes found in Part 6 of the Act.

Further exemptions - Schedule 11

Schedule 11 provides further exemptions which may be applied in specific scenarios.

These exemptions relate to:

- The prevention of crime.
- Information required to be disclosed by law.
- Parliamentary privilege.
- Prejudice to judicial proceedings.
- The conferring by the Crown of any honour or dignity.
- Prejudice to combat effectiveness of any of the armed forces.
- Prejudice to the economic well-being of the United Kingdom.
- Legal professional privilege.
- Prejudice to negotiations with the data subject.
- Confidential references given by the controller
- Exam scripts or marks
- Research and statistical purposes
- Archiving in the public interest.

Part 5, Data Protection Act

The Information Commissioner

The Information Commissioner is the UK's national supervisory authority for the purposes of the GDPR, the LED and the Act and shall continue to be the UK's designated authority for the purposes of the Convention 108.

Part 5 with Schedules 12 and 13 ensure that the Information Commissioner and her office continue to operate and list some of the Information Commissioner's functions, duties and powers.

The Information Commissioner has issued a Regulatory Action Policy, setting out how the Commissioner proposes to exercise her functions, duties and powers.

Part 6, Data Protection Act

Enforcement

What is the scope of Part 6?

Part 6 of the Act relates to enforcement and addresses a wide range of areas.

When reading Part 6 of the Act there is a logical progression, from considering the Information Commissioner's civil enforcement powers, which are exercisable through a series of notices, the effects of which are summarised in the table found on the next page, through to explaining what action a person can take against such notices.

Part 6 also considers complaints made by individuals, the potential remedies that can be provided by a court including compliance orders and compensation to data subjects (which may be awarded for contravention of the GDPR or other data protection legislation).

Finally Part 6, and some provisions found within Part 7, address a variety of criminal offences and their penalties.

Information Commissioner enforcement actions and rights of appeal
Part 6, Sections 142 to 164

The Information Commissioner's powers under Part 6 of the Act apply to data processing activities that fall under the GDPR, the applied GDPR Part 3, Chapter 2of the Act (law enforcement processing) and Part 4, Chapter 2 of the Act (intelligence services processing).

Type of notice	Information Notice (Sections 142-145)	Assessment Notice (Sections 146-147)	Enforcement Notice (Sections 149-153 and Schedule 15)	Penalty Notice (Sections 155-159 and Schedule 16)
What is the purpose of the notice?	To require someone to provide information that the Commissioner reasonably requires for her functions or for certain investigations.	To require a controller or processor to submit to an assessment as to data protection compliance.	To require a person to take the steps specified in the notice, or to require that a person refrains from taking certain steps.	To require a person to pay to the Commissioner the amount specified in the notice.
When can a notice be issued?	As part of the Information Commissioner's exercise of its investigative powers. For more information, see our Regulatory Action Policy.	As part of the Information Commissioner's exercise of its investigative powers. For more information, see our Regulatory Action Policy. Where a notice is given to a processor – the Commissioner must provide a copy to each relevant controller if reasonably practicable.	In simple terms, when a person has failed to comply with its obligations under the GDPR, the Act, or the fees regulations. For more information, see our Regulatory Action Policy.	In simple terms, when a person has failed to comply with its obligations under the legislation, or failed to comply with an information notice, assessment notice, or enforcement notice. The Commissioner must issue a 'notice of intent' first. For more information, see our Regulatory Action Policy.

Type of notice	Information Notice (Sections 142-145)	Assessment Notice (Sections 146-147)	Enforcement Notice (Sections 149-153 and Schedule 15)	Penalty Notice (Sections 155-159 and Schedule 16)
What must the notice contain?	• Reference to the subsection within s142 of the Act the Commissioner is relying on to issue the notice. • Why the Commissioner requires this information. • The consequences of failing to comply with the notice. • Information about rights of appeal. It must not require information to be provided before the end of the appeal period, unless the matter is urgent.	• The time, or period for compliance. • The consequences of failing to comply with the notice. • Information about rights of appeal.	• Details of the failures and reasons for reaching such an opinion and the steps to be taken and/or refrained from being taken. • The consequences of failing to comply with the notice. • Information about rights of appeal.	The notice of intent must include: • why the Commissioner proposes to issue the penalty notice; • an indication of the amount and aggravating or mitigating factors; and • the right to make representations, how to do so, and the period in which they can be made. The penalty notice must include: • whether representations were made; • reasons for the penalty and the amount; • how it is to be paid; • information about rights of appeal.

6 Part 6, Data Protection Act

Type of notice	Information Notice (Sections 142-145)	Assessment Notice (Sections 146-147)	Enforcement Notice (Sections 149-153 and Schedule 15)	Penalty Notice (Sections 155-159 and Schedule 16)
When does a person not need to comply?	• Where the information is legal advice or other communications between lawyer and client about compliance with or proceedings under data protection law. • Where providing the information would infringe the privileges of either Houses of Parliament. • Where doing so would reveal evidence of the commission of certain offences. • If they appeal, until the appeal has been determined or withdrawn • Where the notice is withdrawn in writing.	• Where the information is legal advice or other communications between lawyer and client about compliance with or proceedings under data protection law. • Where providing the information would infringe the privileges of either Houses of Parliament. • Where personal data is being processed for the special purposes. • If the person is specified in section 147(6)(a) or (b) (eg a Security Service). • If they appeal, until the appeal has been determined or withdrawn. • Where the notice is withdrawn in writing.	• Where providing the information would infringe the privileges of either Houses of Parliament. • Where the processing is for the special purposes, unless the Commissioner has issued a s174 determination and the court has granted leave for the notice. • Where, under Part 3 or Part 4, a person is a joint controller not responsible for compliance with the relevant provision. • If they appeal, until the appeal has been determined or withdrawn. • Where the notice is withdrawn in writing.	• If that person is the Keeper of the Privy Purse, the Crown Estate Commissioners, or a controller for the Duchies of Lancaster or Cornwall • Where the controller is either House of Parliament • Where the processing is for the special purposes, unless the Information Commissioner has issued a s174 determination and the court has granted leave for the notice. • Where, under Part 3 or Part 4, a person is a joint controller not responsible for compliance with the relevant provision. • Where the notice is withdrawn in writing.

6 Part 6, Data Protection Act

Type of notice	Information Notice (Sections 142-145)	Assessment Notice (Sections 146-147)	Enforcement Notice (Sections 149-153 and Schedule 15)	Penalty Notice (Sections 155-159 and Schedule 16)
When must a notice be complied with?	• The period in which a penalty must be paid will be detailed in the notice. • This must be after the time to appeal has expired, unless the notice is urgent and reasons are given. The minimum amount of time to comply must still be at least 24 hours.	• The period in which a penalty must be paid will be detailed in the notice. • This must be after the time to appeal has expired, unless the notice is urgent and reasons are given. The minimum amount of time to comply must usually still be at least 7 days (unless there are reasonable grounds to suspect a failure to comply with certain provisions, or commission of an offence).	• The period in which a penalty must be paid will be detailed in the notice • This must be after the time to appeal has expired, unless the notice is urgent and reasons are given. The minimum amount of time to respond must still be at least 24 hours.	• The period in which a penalty must be paid will be detailed in the notice. • This must be at least 28 days from the date the notice was given. • The Commissioner must not take action to recover the penalty unless the time to appeal has expired and any appeals have been decided or ended.
What happens if a person fails to comply with a notice?	• A penalty notice. • It is an offence to make a statement you know is false or recklessly make a statement which is false in a material respect. • The Commissioner may apply to the court to require compliance	• A penalty notice. • Failure to comply may lead to the issue of a warrant for entry and inspection.	• A penalty notice.	• The Commissioner may apply for a Court Order (in England and Wales or Northern Ireland) or a warrant for execution (in Scotland).

Monetary penalties that the Information Commissioner may impose
Part 6, Sections 157 to 159

The maximum penalty that may be imposed depends on the reason for the penalty notice, and is either:

- "the **standard maximum amount**": the higher of 10,000,000 EUR or (in the case of an undertaking) 2% of the undertaking's total annual worldwide turnover in the preceding financial year.
- "the **higher maximum amount**": the higher of 20,000,000 EUR or (in the case of an undertaking) 4% of the undertaking's total annual worldwide turnover in the preceding financial year.

The Act specifies the following maximum penalties for infringements:

Higher maximum amount	• Failure to comply with an information, assessment or enforcement notice. • Failure to comply with sections 35 to 37, 38(1), 39(1), 40, 44 to 49, 52, 53, 73, or 74 to 78 of Part 3 of the Act. • Failure to comply with sections 86 to 91, 93, 94, 100 or 109 of Part 4 of the Act. • Failure to comply with provisions of the GDPR which are specified in Article 83 as subject to the higher maximum amount.
Standard maximum amount	• Other infringements of the GDPR, or Part 3 or 4 of the Act

Powers of entry and inspection (search warrants)
Part 6, Section 154 and Schedule 15

A warrant may be issued if a court judge is satisfied that there are reasonable grounds to suspect that crime under the Act has been or is being committed, or that a person has failed, or is failing, to (in summary):

- comply with the data protection principles, data subject rights and controller/processor obligations set out in the GDPR or the Act;
- communicate a personal data breach to the Information Commissioner or a data subject; or
- comply with the principles for transfers of personal data to third countries, non-Convention countries and international organisations.

(This list is initially set out in Section 149(2)). In addition, a judge must also be satisfied that there are reasonable grounds to suspect that evidence of the failure or offence can be found on the premises, or could be viewed using equipment on the premises)

In addition, should a person fail to comply with an Assessment Notice the Information Commissioner may apply to the court for a warrant, to enable her to determine if the controller or processor has or is complying with the data protection legislation..

There warrant will not be issued unless the Information Commissioner has complied with a number of conditions unless compliance with them would defeat the object of entry, or access is required urgently:

Condition 1

- At least seven days have passed since the Information Commissioner gave notice in writing demanding access to the premises in question.

Condition 2

- Access was demanded at a reasonable hour, but access was unreasonably refused; or
- Entry was granted by the occupier, but they unreasonably refused to allow the Information Commissioner to carry out the required searches and inspections.

Condition 3

- The occupier of the premises was notified by the Information Commissioner that an application for the warrant had been made; and

- The occupier had an opportunity to be heard by the judge on the question of whether the warrant should be issued or not.

Condition 4

- If the personal data are processed for the special purposes, a determination under s174 of the Act has taken effect.

The powers of inspection and seizure conferred by a warrant are not exercisable in relation to:

- information that consists of a communication between legal adviser and client in respect of advice to the client regarding compliance with the data protection legislation or
- information consisting of a communication between legal adviser and client or between legal adviser and client and another person in connection with, and for, proceedings relating to the data protection legislation, or
- where their exercise would infringe the privileges of either House of Parliament.

Further details as to what the warrant should contain and how it operates are in Schedule 15 of the Act.

It is also important to note that it is an offence to intentionally obstruct the execution of a warrant, or to fail to offer assistance that may be reasonably required, without reasonable grounds to do so.

Rights of appeal and Determinations of appeals
Part 6, Sections 162-163

A person may appeal the following to the Tribunal:

- An information notice.
- An assessment notice.
- An enforcement notice.
- A penalty notice.
- A penalty variation notice.
- The amount of a penalty specified in a penalty or penalty variation notice.
- The urgency of compliance with any of the above notices required by the Information Commissioner.
- A refusal by the Information Commissioner to cancel or vary an enforcement notice.

- A determination made under s.174 of the Act.

The provisions on appeals to the Tribunal are largely unchanged. This means that the Tribunal may review the facts and circumstances of the case and the legal basis, and may substitute its own decision for that of the Information Commissioner.

Complaints by data subjects
Part 6, Section 165

Section 165 requires the Information Commissioner to deal with complaints about data processing that are made by data subjects in relation to infringements of Parts 3 and 4 of the Act.

The Information Commissioner must take appropriate steps when responding to such a complaint. This includes carrying out an investigation and providing the data subject with information about progress made, including whether further investigations will be required. Additionally, the Information Commissioner must inform the data subject of the outcome of the complaint; provide information about appeals; and, if asked to do so, provide further information about how to pursue the complaint.

If a complaint relates to an alleged infringement of an individual's rights under another EU country's laws implementing the Law Enforcement Directive, the Information Commissioner must send the complaint to the supervisory authority in that other country. The Information Commissioner must inform the individual that the complaint has been passed on, and, if requested, provide further information about how the individual can pursue the complaint.

Orders to progress complaints
Part 6, Section 166

Section 166 provides an additional mechanism for an individual to progress a complaint made in relation to processing under Parts 2 to 4 of the Act. Should they be unhappy with how the Information Commissioner has handled their complaint, they may, in certain circumstances, apply to the Information Tribunal.

The Information Tribunal has the power to order the Information Commissioner to take appropriate steps to respond to the complaint and to inform the complainant of the progress made, or the outcome, within a specified period.

Compliance orders
Part 6, Section 167

Section 167 guarantees an individual the right to an effective judicial remedy against non-compliance with the GDPR or Parts 2 and 3 of the Act by a controller

or processor.

This provides that an individual may bring court proceedings, in addition to, or as an alternative to, making a complaint to the Information Commissioner. The court has the power to order the controller or processor to take specified steps, or refrain from taking specified steps, for the purposes of securing compliance. However, the court must specify the period within which a step should be taken, or the time at which a step should be taken.

If the court proceedings concern joint controllers who are undertaking processing activities in accordance with Part 3 of the Act, the court can only order a particular controller to take or refrain from taking steps if it is satisfied that the particular controller is responsible for the compliance issue that the case involves.

Compensation for contravention of the GDPR
Part 6, Section 168

Section 168 provides that court proceedings for compensation under Article 82 GDPR, can include a claim for distress Claims can be brought by a representative body on behalf of a person and compensation paid to the person, the representative body, or such other person as the court thinks fit.

Compensation for a contravention of other data protection legislation
Part 6, Section 169

Section 169 provides that a person who suffers damage following a contravention of data protection legislation, other than that of the GDPR, may also be entitled to compensation. For these purposes, damage means financial loss, or distress. Compensation proceedings can be brought against controllers and processors.

A controller will not be liable for the damage or distress if it can prove that it was not responsible for the event that gave rise to the damage complained about. Processors are only liable for damage caused by their failure to comply with their processing obligations, or if they have acted beyond the scope of their instructions. However, like controllers, they will be exempt from liability if they can prove that they were not responsible for the event that gave rise to the damage.

Joint controllers, who are caught by the provisions of Parts 3 or 4 of the Act, will only be liable where they are responsible for compliance with the area of data protection legislation which they have fallen foul of.

Destroying of falsifying information and documents etc
Part 6, Section 148

Section 148 applies where a person has been given an information notice or assessment notice which requires that certain information is provided to the Information Commissioner or requires them to direct the Commissioner to documents, equipment or material.

In this situation it is an offence for that person to intend to prevent the Information Commissioner from accessing the requested information or documents, equipment or material by destroying or otherwise disposing of, concealing, blocking or falsifying the information and documentation etc. It is also an offence to cause or permit these actions.

However, it will be a defence if the person can prove that the destruction or disposal etc would have occurred regardless of the notice being given.

The unlawful obtaining of personal data
Part 6, Section 170

Section 170 sets out a series of criminal offences related to the unlawful handling of personal data. It is an offence to knowingly or recklessly:

- obtain or disclose personal data without the consent of the controller;
- procure the disclosure of personal data to another person without the consent of the controller; or
- after it has been obtained, to retain personal data, , without the consent of the person who was controller when it was obtained.

Defences include:

- The action was necessary for the purposes of preventing or detecting crime.
- The action was required or authorised by an enactment, rule of law or court or tribunal order.
- The action was justified in the public interest.
- The person acted in the reasonable belief that their action was lawful or that the controller would have consented, had they known what has happening.
- The person acted for the special purposes, with a view to the publication by a person of any journalistic, academic, artistic or literary material, and in the reasonable belief that in the particular circumstances the action was justified as being in the public interest.

It is also an offence to sell, or offer to sell personal data that has been unlawfully obtained, which includes advertising this data for sale.

Re-identification of de-identified personal data
Part 6, Sections 171 and 172

Sections 171 and 172 detail two criminal offences relating to the re-identification of de-identified personal data.

Personal data is de-identified if it is processed in a way that means that it cannot be attributed to a specific person without further steps being taken. Re-identification occurs when such steps are taken.

It is an offence:

- if a person knowingly or recklessly re-identifies de-identified personal data without the consent of the controller who de-identified the personal data; or
- if a person knowingly or recklessly processes personal data that has been re-identified (which was an offence), without the consent of the controller responsible for the de-identification.

However, there are a series of defences. In general these are similar to those found under section 170 for the unlawful obtaining of personal data.

There is a specific defence for re-identification to test the effectiveness of de-identification, if both 'effectiveness testing conditions' are met:

> Condition 1: The person was testing the effectiveness of the de-identification systems used by other controllers, which they reasonably believe is justified as being in the public interest, and where they do not intend to cause or threaten damage or distress.
>
> Condition 2: The person notified the Information Commissioner or controller responsible for de-identifying the personal data about the re-identification, without undue delay, and where feasible, not later than 72 hours after becoming aware of it.

Where there is more than one controller responsible for de-identifying personal data, Condition 2 will be met should one or more of the controllers be notified.

The alteration of personal data to prevent disclosure to the data subject

Part 6, Section 173

Section 173 provides that, where a subject access or data portability request has been received, it is an offence for a controller or related persons, including a processor, to take action to prevent the provision of information which an individual would be entitled to receive.

It is a defence if the action would have occurred regardless of the request or if the person charged acted in the reasonable belief that the individual was not entitled to receive the information.

Provisions relating to the special purposes

Part 6, Sections 174 to 176

What are the special purposes?

Sections 174-176 provides specific derogations from the GDPR for the following purposes:

- Journalistic
- Academic
- Artistic
- Literary

These derogations are permitted in accordance with Article 85(1) of the GDPR, which acknowledges that freedom of expression is a fundamental right along with the right to data protection. These derogations are defined as the 'special purposes'.

What are the Information Commissioner's powers in relation to the special purposes?

Where an organisation claims that it is processing for the special purposes, the Information Commissioner may determine, in writing, that:

- the personal data is not being processed only for the special purposes; or
- the personal data is not being processed with a view to the publication by a person of journalistic, academic, artistic or literary material which it has not previously published.

The Information Commissioner must provide this written determination to both the controller and processer. Such notice must also provide information about rights of appeal.

When will this determination take effect?

This written determination will not take effect until the period in which an appeal could be brought has passed, or, if the appeal has been brought it has been decided or otherwise ended and no further appeal can be brought.

How the Information Commissioner can help, should an individual be a party to proceedings relating to these special purposes?

The Information Commissioner can offer help to an individual who applies for assistance, who is a party, or prospective party to special purposes proceedings.

"Special purposes proceedings" are legal proceedings against a controller or processor relating wholly or partly to processing for the special purposes and are proceedings as set out in s167 or 169 of the Act (proceedings for a compliance order or compensation for a contravention of non GDPR processing) or Articles 79 or 82 of GDPR

The Information Commissioner will respond as soon as practicable confirming whether she can assist. She can only assist if the case involves a matter of substantial public importance. Where she can assist she will inform an individual about how much assistance she can provide and will inform the other party against whom the proceedings are brought. If the Information Commissioner is unable to assist, she will notify the individual why.

How can the Information Commissioner assist an individual in special purposes proceedings?

The Information Commissioner can offer a range of assistance such as paying an individual's costs for proceedings or indemnifying them for their liability to pay costs, expenses or damages connected to proceedings.

When will special purpose proceedings be stayed?

A stay of proceedings is a ruling by a court that halts further legal proceedings. Special purposes proceedings will be stayed (or sisted in Scotland) if the controller claims, or it appears to the court, that the personal data:

- are only being processed for the special purposes;
- with a view to any person publishing journalistic, academic, artistic or literary material; and
- they have not previously been published by the controller.

The stay (or sist) will remain in place until the controller or processor withdraws that claim or until a determination made by the Information Commissioner in accordance with s174 of the Act takes effect.

Prohibition of requirement to produce relevant records
Part 7, Section 184

Section 184 protects individuals by making it an offence for a person to require another person to request access to a relevant record. The meaning of a relevant record is provided for within Schedule 18 and includes a health record and records relating to a conviction or caution.

Such a request is not permitted in connection with recruitment or continued employment of an employee or a contract for services.

It is an offence if a person requires another person to make an access request as a condition of providing goods, facilities or services to them or another (which are provided to the public or a section of the public).

It is a defence if the requirement to supply a relevant record was required by an enactment, rule of law or order of the court or was justified in the public interest.

Representation of data subjects with their authority
Part 7, Section 187 and 188

Section 187 provides that a not-for-profit body may, in certain instances, represent an individual in relation to processing under the GDPR applies or outside the scope of the GDPR. This includes in court proceedings for compensation against a controller or processor.

There are certain conditions that attach to the representative body, it must be active in the field of data protection, and be not-for-profit body with objectives in the public interest.

The Secretary of State may also make regulations so that it is possible for representative bodies to bring proceedings before a court or tribunal in England and Wales or Northern Ireland, combining two or more relevant claims.

Penalties for offences
Part 7, Sections 196

Depending upon the offence committed a person may be liable to a range of fines. The amount of these fines are provided for within Section 196.
Section 196 also confirms that in cases relating to the unlawful obtaining and forced disclosure of personal data, that the court can order that materials containing personal data be destroyed.

The prosecuting authorities in England, Wales and Northern Ireland are the Information Commissioner or the Director of Public Prosecutions (the DPP also

has the power to authorise prosecutions by others). Such prosecutions may be brought within a period of six months, beginning from the day the prosecutor first knew of evidence sufficient to bring such proceedings, and must be brought within three years of the offence being committed.

Directors personal liability for offences
Part 7, Section 198

The Act provides for the prosecution of company directors, managers, secretaries, officers and others, as well at the company itself, where an offence by the company is proved to have been committed with their consent, connivance, or neglect. If a company's affairs are managed by its members, they can be personally prosecuted for their acts of omissions.

Recordable offences
Part 7, Section 199

Section 199 lists the crimes fall into the category of 'recordable offences'. These are crimes are recorded on the Police National Computer and which constitute a criminal record.

Version 2
January 2019